# CLAIMS

Sub A1

1. A computer-implemented method for digitally signing data, comprising:

generating a lattice $\mathcal{L}$ having at least one short basis establishing a private key and at least one long basis establishing a public key;

mapping at least the message μ or a concatenation thereof to a message point "x" in n-dimensional space using a function "f" rendering infeasible the possibility of mapping two messages close together in the space; and

using the short basis, finding a lattice point "y" of the lattice $\mathcal{L}$ that is close to the message point "x".

2. The method of Claim 1, further comprising returning at least the message point "x" and the lattice point "y" as a digital signature.

3. The method of Claim 2, further comprising randomizing the function "f".

4. The method of Claim 3, wherein the function "f" is randomized by concatenating the message μ with a random number $\rho$.

5. The method of Claim 1, wherein the function "f" maps the message μ to a point on a grid.

6. The method of Claim 5, wherein the function "f" is collision intractable.

7. The method of Claim 6, wherein the collision intractability of the function "f" is derived from the hardness of lattice problems.

a'

8. The method of Claim 5, wherein the function "f" is not collision intractable.

09547202.041203

9. The method of Claim 1, wherein the function "f" maps at least the message to a point on an auxiliary lattice.

10. The method of Claim 1, further comprising verifying a digital signature at least in part by determining whether a difference between the lattice point "y" and the message point "x" is no more than a predetermined distance.

11. The method of Claim 10, wherein the predetermined distance is related to the number of dimensions in the lattice $\mathscr{L}$.

12. A computer program storage device including a program of instructions for generating a digital signature for a message, the program of instructions including:

computer readable code means for mapping a message μ or a concatenation thereof to a message point "x" in n-dimensional space, the message point "x" being a point of a grid or a point of an auxiliary lattice;

computer readable code means for finding a point "y" of a key lattice $\mathscr{L}$ that is nearby the message point "x"; and

computer readable code means for establishing a digital signature, based at least on the points "x" and "y".

a1

09487502.011900

13. The computer program storage device of Claim 12, wherein the means for mapping uses a function "f" rendering infeasible the possibility of mapping two messages close together in the space, and wherein the means for finding includes using a hard to find short basis of the key lattice $\mathscr{L}$.

14. The computer program storage device of Claim 13, further comprising means for randomizing the function "f".

15. The computer program storage device of Claim 14, wherein the function "f" is randomized by concatenating the message μ with a random number $\rho$.

16. The computer program storage device of Claim 12, wherein the function "f" maps the message μ to a point on a grid, and wherein the function "f" is

collision intractable, the collision intractability being derived from the hardness of lattice problems.

17. The computer program storage device of Claim 12, wherein the function "f" is not collision intractable.

a'

18. The computer program storage device of Claim 13, wherein the function "f" maps at least the message to a point on an auxiliary lattice.

19. A computer system for generating a digital signature of a message μ, comprising:

at least one sender computer including logic for executing method steps including:

mapping the message μ to a message point "x" at which it is not feasible to map any other message;

finding a lattice point "y" that is relatively close to the message point "x"; and

transmitting at least the message μ and the points "x" and "y";

at least one receiver computer receiving the message μ and points "x" and "y" and including logic for executing method steps including:

determining whether a distance between the points "x" and "y" is related in a predetermined way to a predetermined distance, and based thereon determining whether the message μ has been properly signed.

20. The system of Claim 19, wherein the mapping act is undertaken using a function "f" that maps the message point "x" to a point of a grid or of an auxiliary lattice, and further wherein the lattice point "y" is a member of a lattice $\mathscr{L}$, and the finding act is undertaken using a hard-to-find short basis of the lattice $\mathscr{L}$.

21. The system of Claim 20, wherein the acts undertaken by the logic of the sender computer further comprise randomizing the function "f" by concatenating the message μ with a random number $\rho$.

22. The system of Claim 20, wherein the function "f" is collision intractable.

23. The system of Claim 22, wherein the collision intractability of the function "f" is derived from the hardness of lattice problems.

24. The system of Claim 20, wherein the function "f" is not collision intractable.

25. The system of Claim 20, wherein the predetermined distance is related to the number "r" of dimensions in the lattice $\mathscr{L}$.

a'

26. A computer-implemented method for digitally signing data, comprising:

generating a lattice $\mathscr{L}$ having at least one short basis and at least one long basis;

mapping at least the message μ or a concatenation thereof to a message point "x" in n-dimensional space, the message point "x" being an element of a set of spaced-apart points; and

using the short basis, finding a lattice point "y" of the lattice $\mathscr{L}$ that is close to the message point "x".

09526065.031700

27. The method of Claim 26, wherein the mapping is undertaken using a function "f".

28. The method of Claim 27, further comprising randomizing the function "f" by concatenating the message μ with a random number $\rho$.

29. The method of Claim 27, wherein the function "f" maps the message μ to a point on a grid.

30. The method of Claim 29, wherein the function "f" is collision intractable.

31. The method of Claim 30, wherein the collision intractability of the function "f" is derived from the hardness of lattice problems.

a'

32. The method of Claim 29, wherein the function "f" is not collision intractable.

33. The method of Claim 27, wherein the function "f" maps at least the message to a point on an auxiliary lattice.

34. The method of Claim 26, further comprising verifying a digital signature at least in part by determining whether a difference between the lattice point "y" and the message point "x" is no more than a predetermined distance.

35. The method of Claim 34, wherein the predetermined distance is related to the number of dimensions in the lattice $\mathscr{L}$.